Contingent Interception and Information Replacement for Transactions Conducted over Networks

DESCRIPTION

[Para 1] This Application is a continuation of and claims priority under 35 USC §120 to US Application Serial No. 10/794,748, filed March 5, 2004, entitled CONTINGENCY NETWORK ACCESS FOR ACCOUNTS OR INFORMATION, published as US2004/0158526 on August 12, 2004, which claims priority to PCT Application Serial No. PCT/US04/03523, filed February 5, 2004, which claims priority to U.S. patent application Ser. No. 10/359,473 filed Feb. 6, 2003 entitled METHOD PROVIDING CONTINGENCY ACCESS TO VALUABLE ACCOUNTS OR INFORMATION, published as US2004/0158523 on August 12, 2004, all of which are incorporated by reference in their entirety, for all purposes.

[Para 2] The present invention relates to improved and user selected privacy and security for financial and informational transaction conducted over local and wide area networks.

[Para 3] Personal security issues surrounding kidnappings relating to secure accounts and other valuable assets or information have become increasingly difficult as electronic access to accounts and information becomes ubiquitous from not only standard network access points, but home network access, wireless communication devices, and access points

[Para 4] FIG. 1 depicts a simplified block diagram of an account access network system 200 of the prior art. Such a system includes one or more Automatic Teller Machines (ATMS) 10, which are connected through a connection 50 to a network 100 which may include one or more vendor access systems, 110a, 110b, . . . , or simply be able to access the vendor access systems 110a, 110b, . . . , through a network connection, 60a, 60b, . . . The ATM 10 includes a display 11, internal connection bus 12, one or more manual dispensers or inserts 13, a numeric keypad 14, an optional keyboard 15A, specialty buttons 15B, or touchscreen devices 15C, a card insert 16, a dispenser 17, a computer 18 which is connected to the internal bus 11, and a network connector 19. The ATM also may include a security system 40, which includes a monitoring system 20, which usually includes a camera 22. The monitoring system 20 is connected through a convention or digital connector 24, such as a coaxial cable or a digital connection to a security monitor or router 26. The security monitor 26 may be connection to a conventional security display 30 that is watched by a security guard at a security station 31. The monitor 26 may also be connected to an analog or digital recorder 29, which records the events before the camera 22 on analog or digital media

35. The security system 40 may also include a panic button 2 or panic speaker/microphone 4 located on the ATM 10. Both the panic button 2 and speaker/microphone 4 may be connected to the security station 31, through a dedicated connection 5, or to a security network 6, which may an outside security system 98, such as contacting the authorities or a third party security company. In some security systems 40, the monitor 26 may be connected to a digital monitor and decision making device 27 which automates the observation through the camera 22 and detects when a problem event is taking place. However this technology is still in development.

[Para 5] Each vendor access system 110a, 110b, . . . includes a network connection 60a, 60b, . . . , a computational system 140a, 140b, . . . Each computational system 140a, 140b, . . . may include one or more general purpose of specialized microprocessors 150a, 150b, and data storage 160a, 160b, . . . Each vendor access system 110a, 110b, . . . may itself include a sub-network 120a, 120b, . . . to connect multiple vendor access systems for a single vendor or multiple vendors. In such a case a single sub-network 120a, 120b, may overlap with a main network 100 or other subnetworks. The ATM 10 may be locally connected to a vendor access system 110a, by a local connection 55. Usually, these situations are the use of intrabank ATMs or where the user's account matches the owner of the ATM (or there is a cooperative system).

[Para 6] A user of the ATM 10 inserts an account card in the card insert 16, and is then prompted for a PIN by the display 12. The PIN is entered on the keypad 14. Depending on the particular configuration of the ATM 10, the user may be allowed to continue the banking transaction, even if the PIN is incorrect. The PIN and other transaction information are entered into input devices 15A, B, or C. The information from the account card may be processed by the ATM processor 18. The PIN and account information are sent to a network 100 via a communication device 19 and a network connection 50. A network 100 may be a large conglomerate of access networks or an individual system such as CIRRUS(R), PLUS(R), or MOST(R). Most consumers will have more that one network accessed by their account card. As can be appreciated by those skilled in art, networks 100 may include many different discrete and overlapping configurations.

[Para 7] The PIN and the account information is properly routed to the appropriate subnetwork 120a, 120b,... where the information is processed by a vendor access system 110a, 110b,... Input PINs may be compared by the computational system 140a, 140b, to the correct PIN for the account in data storage 160a, 160b. Incorrect PINs will be reported back through the network 100 to the ATM processor 18 which will then terminate the transaction or prompt the user for another PIN. Other situations based on the information in storage 160a, 160b,..., such as account balance, daily withdrawal limits, holds, etc. may also terminate the transaction. Where a PIN is correctly entered and a successful transaction occurs, the account information is

usually allowed to pass through the network 100, but not always. Such information may not be available where an ATM 10 is used which is not part of a particular network 100, even though cash may be accessed by the user.

[Para 8] The number of kidnappings in related to "ATM hijackings" is exponentially rising. For example, in one location "false" cab drivers will take tourists to ATM machines and require them to withdraw all the funds available to them under threat of bodily harm or death. After obtaining money, the kidnappers may leave the tourist alone, or upon finding out they have more money available to them the next day, will simply hold the tourist for an indefinite period until the account is drained. [Many banks have a "daily limit" on ATM can help prevent fraud or waste. However, kidnappers who come to know that an individual has $10,000 in a checking account and a daily limit of $500 will be more tempted to either hold the individual until more money is withdrawn, either harm or blackmail the individual (i.e. threaten, stalk) until the money has been delivered or in a worst case scenario torture the victim for their PIN.

[Para 9] Monitoring an account may be helpful to prevent fraud over the course of hours or days. This prior art technology is based on the principle that "unusual" activity will trigger a Bayesian logic program. Often a bank or credit card company will call a customer to confirm that the unusual activity has been authorized. Furthermore, the increasing ubiquity of PINs and passwords for access in daily life for more than just conventional ATMs makes an increasing number of PIN users susceptible to "hijackings" of all sorts, including Internet-accessed accounts and information and security checkpoints of all sorts, of which, may include national defense situations. Also, It is well-known that individuals who are under distress may attempt to reach authorities for "help" at heightened risk to their personal safety, whether the situation be involved a personal risk because of the anger of the bad actor directed to the victim, or because authorities are often not properly trained to deal with such situations.

[Para 10] While Personal Identification Numbers (PINs) have been in mainstream use since the wide implementation of the Automatic Teller Machine (ATM) in the mid 1970s, other, biometrically-related access systems are now coming into the mainstream with the improved availability of scanning and recognition devices. Such access systems include voice printing, retinal scanning, finger/palm print scanning and more. Other types of access devices which have become widespread are related to the Internet and/or telephonic access to a system which usually require entry of passwords and/or PINs.

[Para 11] Other security measures have been tried to prevent danger to a consumer, such as cameras located on ATMs, panic buttons, emergency speakers, etc. These have limitation and dangers, as they may be useful after the fact or notify an observant bad actor that an "alarm" has been set, which may provide great risk to the consumer. Personal security devices may be connected to cellular of PCS telephones,

and may also use GPS or other locating devices, however, these are purely "notification" devices at present and are not combined with systems that protect valuable assets. Also, such systems are expensive. Secure information acquires over the Internet usually requires one or more passwords.

[Para 12] An invention is needed which provides instant contingency protection for valuable assets or personal information that alleviates high-risk situations while not allowing an observing bad actor to realize that such contingency protection is taking place.

[Para 13] The present invention to provide a system which allows a user to implement contingency plans discretely without notice to a potential bad actor or observer. In a preferred embodiment a user is provides a contingency security code which is unrecognizable to an observer who thinks that a transaction is proceeding normally In a preferred embodiment, the contingency code is usually an easily remembered variation of a user's ATM PIN, but is not easily recognizable to the observant bad actor.

[Para 14] The present invention to allow implementation at local and network levels to provide additional security for entities that may not participate in the contingency safety program. The invention allows for entry of the contingency system into a network by having different physical embodiments. For example, in a large system with multiple vendors (such as banks) in which there is only one participant, the system can be inserted without disruption to the network.

[Para 15] The present invention creates a fictitious "scenario" which allows for the consistent appearance that the alternate access scenario is operating normally. Thus, by implementing the contingency code, a user can potentially thwart one or more disastrous results: (1) the observant bad actor is placated and (2) most of the assets, either monetary or informational are protected by the implementation of the contingency code. Optionally, notification of the third party without notice to an observing bad actor may be included as part of the scenario.

[Para 16] The present invention allows for an increasingly complex set of alternate scenarios depending on the desires and circumstances of a user. It is recognized that the field of personal safety is an uncertain one, and any give user may have preferences based on strengths or experiences. This present invention allows the user to have flexibility in order to meet the needs of different consumers. The need for the inventive multiplicity of discrete contingency scenarios will likely only increase as information become accessed from more and more electronic entry points. The invention contemplates the need for providing non-alphanumeric contingency implementation as well, such as voice inflections, alternate fingerprints, notifying eye movements, can all be appreciated as implementing the protective contingency code.

[Para 17] The invention can be more easily understood by the following drawings and diagrams, in which:

[Para 18] FIG. 1 represents prior art ATM system, well-known in the art for several decades as it currently may be implemented;

[Para 19] FIG. 2 represents logic at the ATM level for implementing the present invention;

[Para 20] FIG. 3 represents logic at the network level for implementing the present invention;

[Para 21] FIG. 4A represents a logic system in the present invention implemented at the vendor level.

[Para 22] FIG. 4B represents the system in FIG. 4A in which implementation does not require retrofitting or reprogramming at the individual vendor or network level;

[Para 23] FIG. 4C represent the system in FIG. 4A, in which implementation is incorporated into a vendors' access system.

[Para 24] FIG. 5 represents a method for implementing the alternate access scenario in a flow diagram for the systems in FIG. 2;

[Para 25] FIG. 6 represents a method for implementing the alternate access scenario in a flow diagram for the systems in FIG. 3;

[Para 26] FIG. 7 is a flow chart of the invention in a preferred embodiment with various vendor level implementations shown in FIGS. 4A-4C;

[Para 27] FIG. 8 represents a method for implementing the alternate access scenario based on a pre-determined criteria (location);

[Para 28] FIG. 9 represents a flowchart of a complex scenario in an alternate embodiment of the invention based on three different PINs;

[Para 29] FIG. 10 represents a block diagram of the present invention as it may be implemented on an Internet accessible security account, or programmed remotely;

[Para 30] FIG. 11 is a smart card implementation of the invention;

[Para 31] FIG. 12 is a sample method for use in the smart card embodiment;

[Para 32] FIG. 13A is a representation of the conceptual level of the invention as it may be applied across multiple implementations in which implementation generally occurs prior to and as a condition precedent to interception.

[Para 33] FIG. 13B is a representation of the conceptual level of the invention as it may be applied across multiple implementations in which interception generally occurs prior to and as a condition precedent to implementation.

[Para 34] Referring now to FIGS. 13A (and 13B), a conceptual diagram of the invention as it may be applied across multiple implementations for setting contingency scenarios when accessing secure accounts or information or entry. The contingency system 9000 allows data to enter at a data entry point 9001, which may be an ATM, vendor card swipe, internet, or biometric access entry device. The comparison system 9100 may be physically located at one place or virtually in many places and may monitor a WAN or other network for specific data to occur which is part of the detection system 9200, which may be activated routinely or upon the interception of a piece of information. Other detection systems 9200 will be transparent and only activate upon the matching of a specific result when a function is performed such as de-encryption or the like. Thus if contingency data is not place into data device 9001 or comparison system 9100 the function will not match any activation. If the contingency scenario identifier is detected a series of instructions may be loaded either directly or virtually by the contingency implementation loader 9300. The loader 9300 may actually have to search a WAN or other network to find the appropriate instructions, but also may be located in a single place for economy. If conditions are met then the contingency instructions are execute by the physical or virtual contingency execution module 9800 which may provide notification 9900 and output 9999. If conditions have not been met, the contingency scenario which may have been automatically loaded proceeds to non-contingency execution 9700.

[Para 35] Other detection systems will be transparent and only activate upon the matching of a specific result when a function is performed such as de-encryption or the like. This feature is shown in an alternate or complementary route an implementation system 9500 and an interception system 9600 may provide the contingency instructions. However implementation and interceptions may be provided in reverse order without departing from the scope of the invention as shown in FIG. 13B. Skilled artisans will appreciate that the conceptual embodiments of the invention illustrated in FIGS. 13A and 13B are not mutually exclusive and may be combined fully or partially with success.

[Para 36] Referring now to FIG. 2, a simplified block diagram of a preferred embodiment of the invention 2000 is shown. The contingency security system 1000 is implemented at the pre-network 100 or local level and may be used for one or more ATMs 10. The local level contingency security system 1000 includes a decision device 2100, which may include one or more specialized microprocessors 2120 and is connected to the one or more ATMs 10 through a local connection 2010. The decision device 2100 is connected to data storage 2200 by an internal or external bus 2150, as the data storage 2200 can be located in the decision device 2100. The decision device is connected to a network 100 and vendor access systems 110 through a single or multiple network connections 2050. Optionally, a security notification system 1002 is part of the system 1000. The decision device 2100 is connected to a security system 40 or a notification protocol system 2400 by a connection 2020.

[Para 37] Referring now to FIG. 3 the system of the invention in a preferred embodiment is shown. The contingency security system 1000 is located at the network 100 level. The computational part of the system 1001 may be located on a physical decision device 1100 or at nodal points 1101 or virtual spaces 1102 (described below), which is why the system is indicated by dashed lines. The decision device 1100 is similar to that described in FIG. 2 and may include a standard or specialized microprocessor 1120, data storage 1200 and an internal or external connection to the storage 1150. Like shown in FIG. 2, the system 1000 includes a security notification system 1002, which is connects the network 100 to a security system 40 via a data communication line 1020.

[Para 38] Referring now to FIG. 4A, another embodiment of the invention is shown as implemented at the local vendor access system 110a, 110b,... level. FIG. 4B depicts an embodiment in which the invention 1000 may be implemented without disturbing existing access system 110a, 110b,..., by patching on the system inside the vendor access system but where the decision device 3100 is screening PIN and account data for contingency matches before entering the access system computer 140a, 140b,...The embodiment of the contingency system 1000 shown in FIG. 4B has a particular advantage in that the installation can be executed independent of any networks 100, 120a, 120b,... or computational systems 140a, 140b, . . . However, as can be appreciated by those skilled in the art, the data exchange between the decision device 3100 and the computational system 140a, 140b,..., in this embodiment may require some additional patch software, but communication protocols used in data transport should be sufficient for this purpose.

[Para 39] FIG. 4C shows the invention where the decision device 3100 and/or the data storage 3200 is located inside the access computational system 140a, 140b,..., either as software, embedded software, hardware in the form of an ASIC or part of the another specialized microprocessor device. The implementation of the invention inside the computational system can be implemented in several different ways, as can be appreciated by those skilled in the art.

[Para 40] The standard operation of a PIN at an ATM is known in the art and one particular implementation is described in the background section of the application and shown in FIG. 1. Although, as can be appreciated by those skilled in the art of computer networking and security access, the account information can be implemented in ways other than the brief description above.

[Para 41] The present invention may be implemented by the entry of the alternate or contingency security code (also referred to as "alternate PIN"). When the user punches in the alternate PIN on the ATM keypad 16, the account information from the account card is coupled with the alternate PIN and processed by the invention at the local, network, or vendor levels as shown in FIGS. 2, 3 and 4 respectively. While all three

implementations are similar, setting the contingency scenario into motion is slightly different at the respective levels.

[Para 42] The contingency security code is sent with account information (contingency information) to the network 100. In the local implementation shown in FIG. 2, the contingency information is intercepted by the decision device 2100, and compared with account data and contingency data in storage 2200 for possible contingency match. Even non-contingency information passes through the decision device 2100 for comparison. Certain factors which are internal to the contingency code may optionally flag a contingency comparison by the decision device 2100, such a matching first and last digit, a flagged PIN ending like "57" or "11." However, such an internal flag for the contingency code is not needed and only would be used to save computational resources. If a contingency code has not been entered, the transaction may proceed as normal to its conclusion.

[Para 43] If the decision device 2100 detects that a contingency code has been entered, it then loads or executes a contingency scenario. The instructions for executing the scenario may be stored in the local data storage 2200 or programmed into the decision device 2100 or alternately embedded in storage onto the specialized microprocessor 2120 in the decision device 2100 or contained into the hardware itself. In an alternate embodiment, the decision device 2100 is simply the detector of a contingency code and queries the vendor access system 110a, 110b,..., or the network 100 for instructions on the contingency scenario.

[Para 44] The location of the contingency detection system and contingency scenario instructions do not need to be on the same tier (local, network, subnetwork, vendor, etc.) for the implementation of the invention. Data and networking specialists can appreciate that implementation of the invention over a large network over a period of time will present special problems. The invention provides flexibility in implementation, as it is expected that network or multiple network implementation may occur after local or vendor implementation. An examination of the conceptual block diagram in FIG. 11 allows for an understanding of this principle.

[Para 45] The contingency scenario is loaded into the decision device 2100. The transaction data is then changed to comply with the contingency scenario and sent to the network 100. The transaction is processed by the appropriate vendor access system 110a, 110b,..., with the substituted data (withdraw $250 instead of $1000). The transaction data returns to the decision device 2100 through the network 100 and the decision device 2100 executes instructions so that the ATM processor 18 or ATM 10 display the substitute access information on the screen 11 or on a receipt. The general principle is that the account balance will show a negligible amount. But other scenarios such as showing an much larger amount than available are also contemplated by the invention.

[Para 46] The contingency scenario intercepted at the network level 100, by the decision device 1100, will also result in the "substitution" of transaction (inbound) and account (outbound) data. The vendor access system implementation depicted in FIGS. 4A, 4B and 4C will not require substitute data as the transaction and account data are generally being processed at the source of the information.

[Para 47] Because a detection of a contingency security code by the invention will activate a contingency scenario, which may be stored at the local 2200, network 1200, or vendor 3200 levels, one or more contingency factors can implemented. As can be appreciated by those skilled in the art, contingency factors may be stored in a database in the data storage 2200 or internally embedded in the microprocessor 2120. may be controlled in a typical embodiment of the invention and can include, inter alia: withdrawal limit: when this contingency factor is activated only a limited amount of money may be taken from the account until re-verified by the user; notification of balance in account(s): when this contingency factor is activated, the receipt from the ATM shows a small balance in the account; blocked access to other related accounts: when this contingency factor is activated; notification of Authorities or private security company; location of event or a masking of the location of an event through the interception system; proceed with caution notice: puts a third party on notice that a hostile party is still in contact and engagement must proceed with caution.

[Para 48] Of course for other security scenarios accounting other factors may be included and would vary for embodiments of the invention that are not implemented in the ATM use, but may be present in credit transaction, building or information access.

[Para 49] In one embodiment, the invention includes a process for protecting the characteristics of a transaction accessing assets in an account or information which corresponding to an account held by an account custodian, including a credit card account, comprising the steps of: mapping at least one identification code to at least one diversionary identification code; storing this mapping on an intercept system, and where the intercept system is connected to the network and includes data storage and a computer system. When the diversionary identification code is entered into an access device, the diversionary identification code instructs the access device to route the access transaction to the intercept system. Next, when the access transaction is routed to the intercept system, the intercept system compares at least one diversionary identification code to the mapping. If the mapping indicates that the access transaction meets a masking criteria, the access transaction will be processed by the intercept system according to a set of masking instructions. The masking instructions include contacting the account custodian via the network with the masked transaction information.

[Para 50] Variations on the above-described process for protecting the characteristics of a transaction include where one identification code includes at least a

portion of the information included on the encoded magnetic stripe of a card used in financial transactions. Another optional feature is where the masking instructions include processing the transaction according to any instructions processed at the access device, or where the account custodian will record the intercept system as said access device. The intercept device can have a plurality of locations.

[Para 51] The process for protecting the characteristics of a transaction include where the intercept device records the instructions from said access device in an encoded form. The encoded transactions may be decoded only by a password supplied to an account holder.

[Para 52] The environment for the transaction includes the situation where the access device is a POS terminal for a credit card.

[Para 53] In another embodiment, the invention is a system for protecting the identity of a transaction conducted at least partially over a network, which includes: a replacement transaction device in the form of a card with data at least corresponding to account information and a contingency transaction identifier. This embodiment of the invention also includes a proxy transaction system connected to the network. When the replacement transaction device is used, the proxy transaction server is activated and the proxy transaction server contacts an account custodian over a network in order to process the transaction. The transaction is only known via the network to the account custodian through the proxy transaction system.

[Para 54] In another embodiment, the invention includes a method for protecting information available over a network and physically located in storage with an account custodian, where the information is accessed by at least a first security identifier known and entered by a user. The method includes the acts of: providing the user (either through the account custodian or a third-party service) with a second security identifier, where the second security identifier is distinguishable from the first security identifier. When the second security identifier is entered into the network and detected by the account custodian, said account custodian provides access to alternate information, the alternate information is clearly distinguishable from the user's (primary) information, such that it would not be apparent to an observer other than the user that the alternate information is not the user's (primary) information.

[Para 55] This method can be used in a variety of ways, such that the alternate information is a non-secure subset of said information, where the alternate information is fictitious, where access is provided over a WAN, and where the user's information is personal information or account information.

[Para 56] FIGS. 5-7 depict the method implemented by the three embodiments in FIGS. 2-4 respectively. The only difference between the three methods is that the local and network implementations must replace transaction data at steps X5 and Y5 before allowing the transaction to proceed to the vendor access system 110a, 110b,..., if the respective vendor access systems 110a, 110b,..., are not compatible with the data

produced by the detection of a contingency code. Where the invention is implemented at the vendor access system 110a, 110b,...FIG. 7 is the representative method of the various vendor level implementations as shown in FIGS. 4A, 4B and 4C, the information is corrected and exchanged at the vendor level and does not need "masking" in order to protect both the assets and the consumer.

[Para 57] FIG. 8 is a flow chart of the invention used in the following scenario: The individual determines how much would be needed to satisfy the anticipated demands of the kidnapper in one place (L1) or another place (L2). For example, on a trip to L1, there may be generally very little violence after an initial amount is given to the kidnapper, but in a second location L2, the kidnappers will insist on holding the victim until the account has been drained. Wealthy individuals may wish to set the limit of the alternate access scenario to a desired amount which may be considered as an acceptable loss. Credit line access may placate kidnappers or intimidators.

[Para 58] For illustration purposes only, a user's main PIN in this application will be 5995. The alternate security code will be 5911. However any number of characters may be used for both the main PIN and the contingency or alternate security code.

[Para 59] In a second sample scenario, a pedestrian is held up at gunpoint on the street. The assailant forces the pedestrian to go to the nearest ATM and withdraw (all available) cash. Optionally, the pedestrian informs the assailant he has about $500 dollars in his account, but actually has $20,000. Under the observation of the assailant, the pedestrian enters the PIN 5911 and attempts to withdraw $500 in cash, which activates the contingency scenario at the local, network, or vendor access level. The account allows a $500 withdrawal, informs the police of the location of the assault and that caution must be used as a hostage situation may be created. The bank or invention distributes (intentionally false) information to the ATM that the account now has only $14.02 left which either shows up on the screen or the receipt. The assailant leaves with the $500 in cash.

[Para 60] In scenario 3, a user begins to use an ATM for withdrawal, has put in his card but has not punched the PIN, the user notices that suspicious characters are lurking close to the ATM. The user, for safety and preventive reason, punches the 5911 contingency code. The contingency scenario is activated, but no notification to the authorities takes place. The withdraw limit is set at $300. The user withdraws $50 dollars, the display or receipt is prompted such that only $14.02 is left in the account. The user leaves unhindered and the next day resets his account to remove the contingency.

[Para 61] The invention also allows for other contingency plans which may benefit an individual under distress. For example, if a tourist is kidnapped and there is so little money in the account that the tourist fears that they be a victim of violence, the contingency security code will trigger a small credit line which will placate the kidnapper into letter the tourist go unharmed. Of course, the level of sophistication of

the contingency plane may be adjusted according to the sophistication. For example, wealthy individuals may wish to be allowed several different levels of protection. FIG. 9 depicts a flow chart of an example situation in a multiple-scenario contingency system based on multiple PINS.

[Para 62] Referring now to FIG. 10, an Internet embodiment of the present invention 7000 is shown. Typically, the victim will be accosted at home or an office, in which the bad actors will attempt to get resources from the victim. A home or office computer system 7010 is connected to a WAN 7100 through a communication line 7015 or a wireless access system 7016. This contingency scenario system 7000 can be loaded into the computer 7010 or if the computer 7100 is part of a LAN 7090 is attached to a WAN 7100 or the Internet. The system 7000 may also be part of the LAN 7090, located in between the LAN 7090 and the computer 7010 or between the LAN 7090 and the WAN 7100. It is anticipated that for large commercial, industrial, or government settings the most economical location would implemented at the outgoing point 7095 to the WAN, but other installation may be needed as well. The contingency system 7000 located at or on the vendor access system 7200, whether it be a bank or other industrial or government access point. Like the above embodiments, the alternate password or PIN will set in motion a stored contingency scenario. The contingency system 7000 can be located inside the vendor's system 7200 or may be implemented. In other embodiments, the networked account may allow a user to select from a series of executable contingency scenarios if desired. This is like the possible alternate contingency scenarios outlined in FIGS. 8 and 9, above.

[Para 63] FIG. 11A depicts a block diagram of the invention 1000 as it may be implemented in an embodiment of the invention which uses a smart card 4001 which contains the software in a microchip 4005 necessary for the implementation of the invention. Data is loaded from the smart card 4001 inserted in the card slot 16 into the ATM processor 18 and network 100. The decision device 4100 and optional data storage 4200 can be located anywhere in the system 1000. However, as can be appreciated by those skilled in the art, there must be a part of the system 1000 that can interpret instructions loaded from the smart card 4001 and the ATM 10 must have the capacity to load and transfer such instructions to the system 1000. FIG. 12 corresponds to sample steps in the implementation of said smart card embodiment of the invention.

[Para 64] The present invention may easily be adapted to the following other scenarios with departing from the spirit and scope of the invention: Home security (home invasion); Cellular and PCS emergency notification (with or without GPS); Defense and intelligence monitoring and security clearance; commercial and industrial information sharing. Of course, vendors would have the option to implement more complex scenarios if so desired, but in no event should the alternate security code have any identifying characteristics to a hostile observer.

[Para 65] The present invention as may be used in a biometric access system (not shown). This embodiment includes one or more biometric detectors, a decision device which includes a general or specialized microprocessor, connected to the detector through a local or network connection, and data storage. The connection to the scenario generator and/or notification system can be through a conventional connection. This alternate embodiment may be implemented in a voice recognition access system, where voice fluctuations or other variation notify a contingency detection system of a contingency situation; in a retinal scanning device, where particular eye movements activate the contingency scenario; or implemented in a finger or palm print recognition device where the angle of the main finger activates the contingency scenario.

[Para 66] The above illustrations are meant to representative only and the spirit and scope of the invention may be applicable for other applications. The invention should be defined by the following claims.